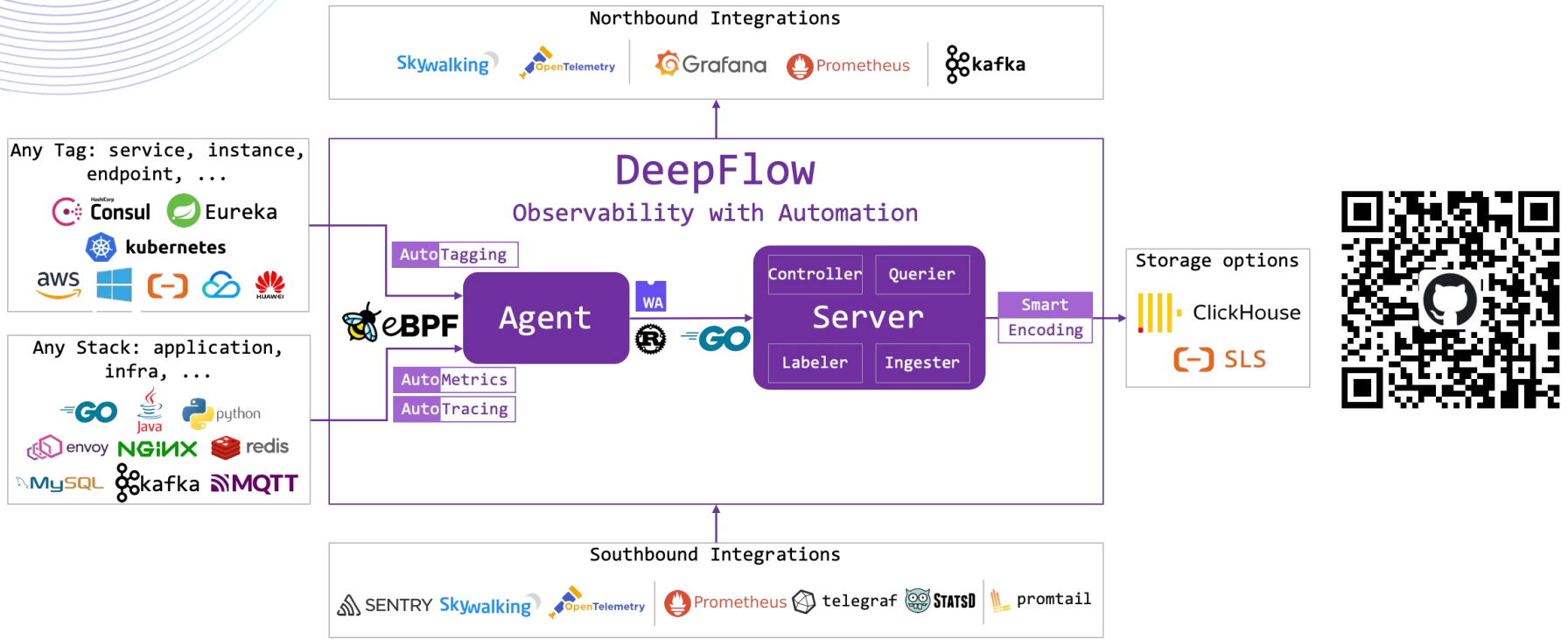
DeepFlow AutoLogging: 自动采集应用调用日志和流日志

李倩 / 云杉网络 产品专家

2022年8月17日

DeepFlow 开源版本



https://deepflow.yunshan.net/blog/001-a-new-era-of-automated-observability/

内容目录

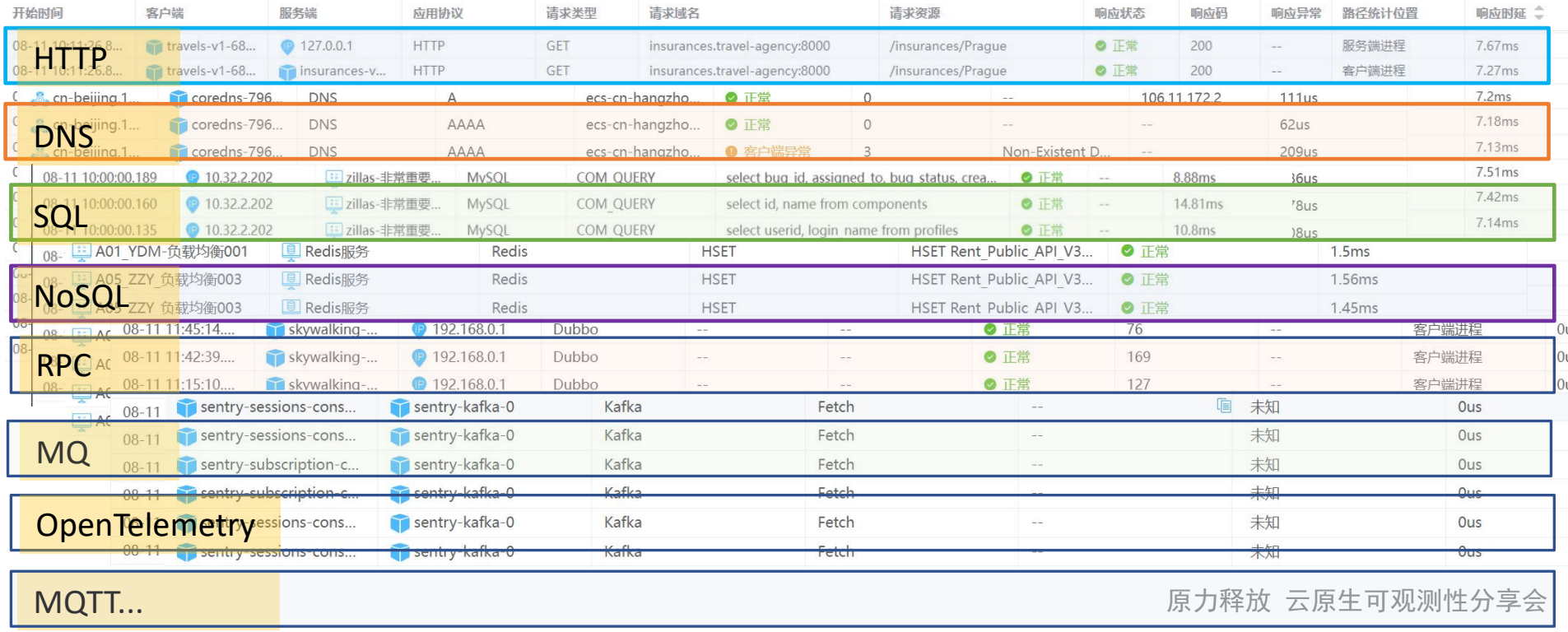
应用调用日志，自动采集HTTP/MySQL等多协议调用日志

网络流日志，丰富指标量及TAG增强网络可观测性

AutoLogging，基于 BPF/eBPF的自动日志采集能力

应用调用日志-数据来源

给Dev团队建设的一个站在应用视角快速查看所有的调用详情信息的一个能力



应用调用日志-数据抽象

公共字段	应用协议 (l7_protocol)	HTTP	MySQL	DNS
	协议版本 (version)	1.0/1.1/2	5.6+	all
	日志类型 (type)	请求/响应/会话	请求/响应/会话	请求/响应/会话
请求字段	请求类型 (request_type)	method	command_type	qurey_type
	请求域名 (request_domain)	host	--	
	请求资源 (request_resource)	path	command	qurey_name
	请求ID (request_id)	stream_id	--	transaction_id
响应字段	响应状态 (response_status)	根据status的官方定义设定	根据response packets定义	根据reply_code的官方定义设定
	响应码 (response_code)	status	error_code	reply_code
	响应异常 (response_exception)	根据status的官方定义设定	error_message	根据reply_code的官方定义设定
	响应结果 (response_result)	--	--	answer
指标量	请求长度 (request_length)	content-length	--	--
	响应长度 (response_length)	content-length	--	--
	响应时延 (response_duration)	response_time - request_time	response_time - request_time	response_time - request_time

Redis

Dubbo

Kafka

MQTT

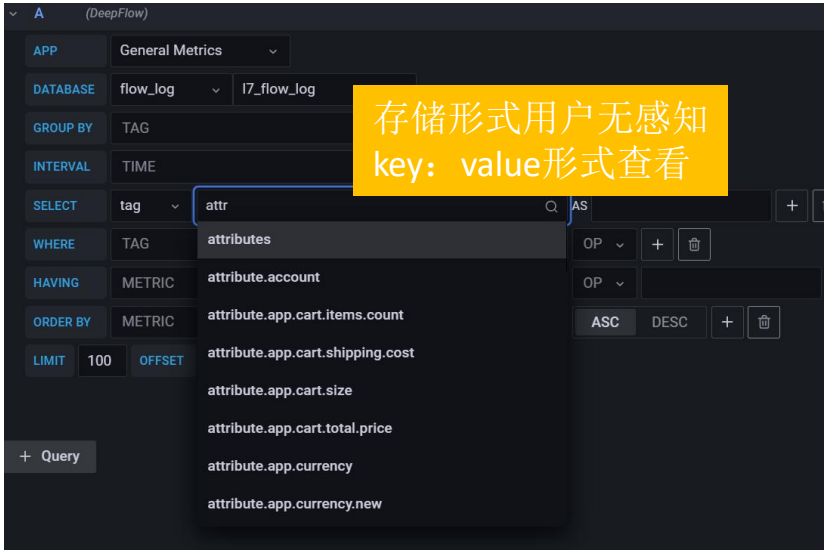
OpenTelemetry

...

应用调用日志-自定义属性

category	keyName	column1_value
原始Attribute	container.id	197bdb26fca4aac843387
原始Attribute	host.arch	amd64
原始Attribute	host.name	web-shop-5cb6479d7b-d
原始Attribute	http.flavor	1.1
原始Attribute	http.host	web-shop:8090
原始Attribute	http.method	GET
原始Attribute	http.route	/shop/full-test
原始Attribute	http.scheme	http
原始Attribute	http.status_code	200
原始Attribute	http.target	/shop/full-test
原始Attribute	http.user_agent	python-requests/2.27.
原始Attribute	k8s.pod.ip	172.17.114.216
原始Attribute	net.peer.ip	172.17.96.103
原始Attribute	net.peer.port	47146
原始Attribute	net.transport	ip_tcp
原始Attribute	os.description	Linux 5.4.205-1.el7.e
原始Attribute	os.type	linux
原始Attribute	process.command_line	/usr/lib/jvm/java-1.8
原始Attribute	process.executable.path	/usr/lib/jvm/java-1.8
原始Attribute	process.pid	7
原始Attribute	process.runtime.description	IcedTea OpenJDK 64-Bi
原始Attribute	process.runtime.name	OpenJDK Runtime Envir
原始Attribute	process.runtime.version	1.8.0_212-b04

```
`attribute_names` Array(String) COMMENT '自定义属性',
`attribute_values` Array(String) COMMENT '自定义属性对应的值'
```



应用调用日志-AutoTagging

计算/网络

category	keyName
知识图谱	region_0
知识图谱	region_1
知识图谱	az_0
知识图谱	az_1
知识图谱	host_0
知识图谱	host_1
知识图谱	chost_0
知识图谱	chost_1
知识图谱	vpc_0
知识图谱	vpc_1
知识图谱	l2_vpc_0
知识图谱	l2_vpc_1
知识图谱	subnet_0
知识图谱	subnet_1
知识图谱	router_0
知识图谱	router_1
知识图谱	dhcpgw_0
知识图谱	dhcpgw_1
知识图谱	lb_0
知识图谱	lb_1
知识图谱	natgw_0
知识图谱	natgw_1
知识图谱	redis_0

存储

category	keyName
知识图谱	redis_0
知识图谱	redis_1
知识图谱	rds_0
知识图谱	rds_1

容器

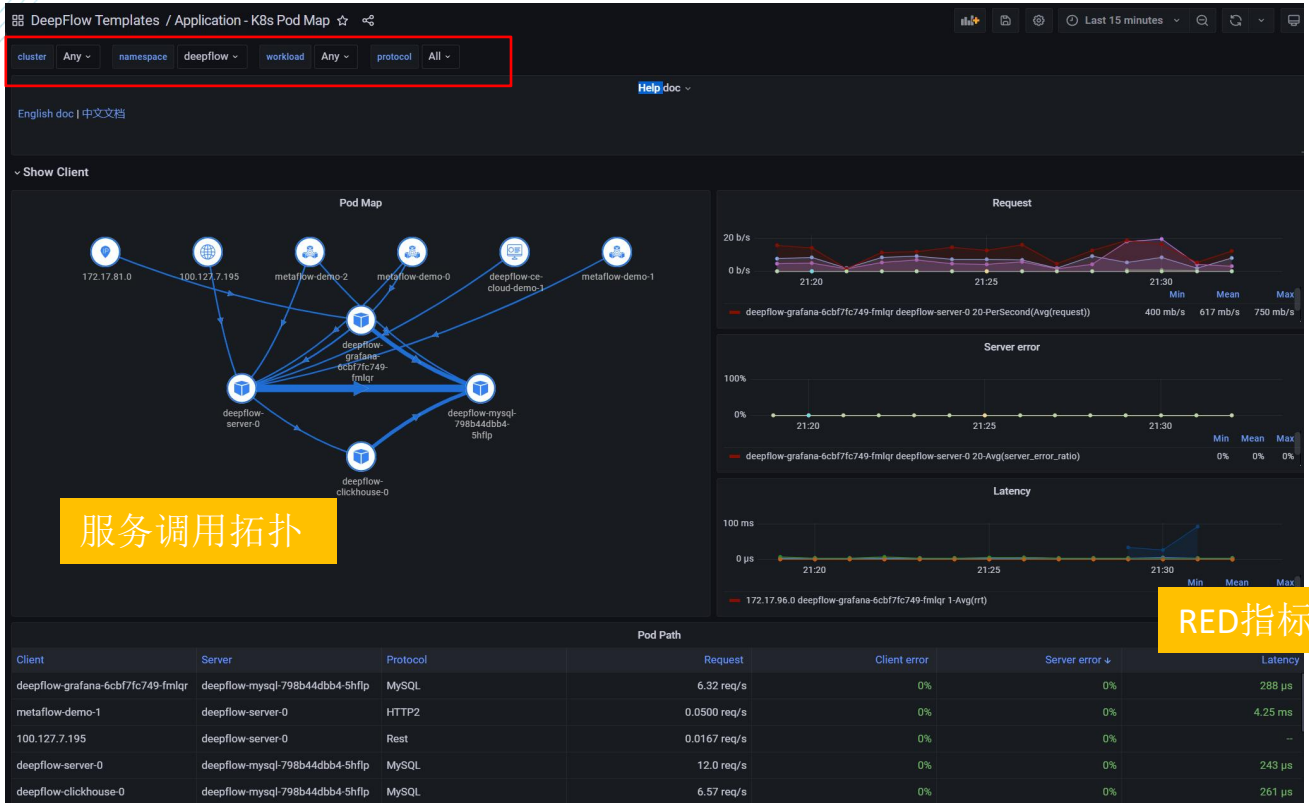
category	keyName
知识图谱	pod_cluster_0
知识图谱	pod_cluster_1
知识图谱	pod_ns_0
知识图谱	pod_ns_1
知识图谱	pod_node_0
知识图谱	pod_node_1
知识图谱	pod_service_0
知识图谱	pod_service_1
知识图谱	pod_group_0
知识图谱	pod_group_1
知识图谱	pod_0
知识图谱	pod_1

K8s标签

category	keyName
标签	label.version_0
标签	label.version_1
标签	label.release_0
标签	label.release_1
标签	label.k8s-app_0
标签	label.k8s-app_1
标签	label.chart_0
标签	label.chart_1
标签	label.heritage_0
标签	label.heritage_1
标签	label.istio_0
标签	label.istio_1
标签	label.app_0
标签	label.app_1
标签	label.role_0
标签	label.role_1
标签	label.name_0
标签	label.name_1
标签	label.istio.io/rev_0
标签	label.istio.io/rev_1
标签	label.helm.sh/chart_0
标签	label.helm.sh/chart_1
标签	label.component_0

应用调用日志-总览

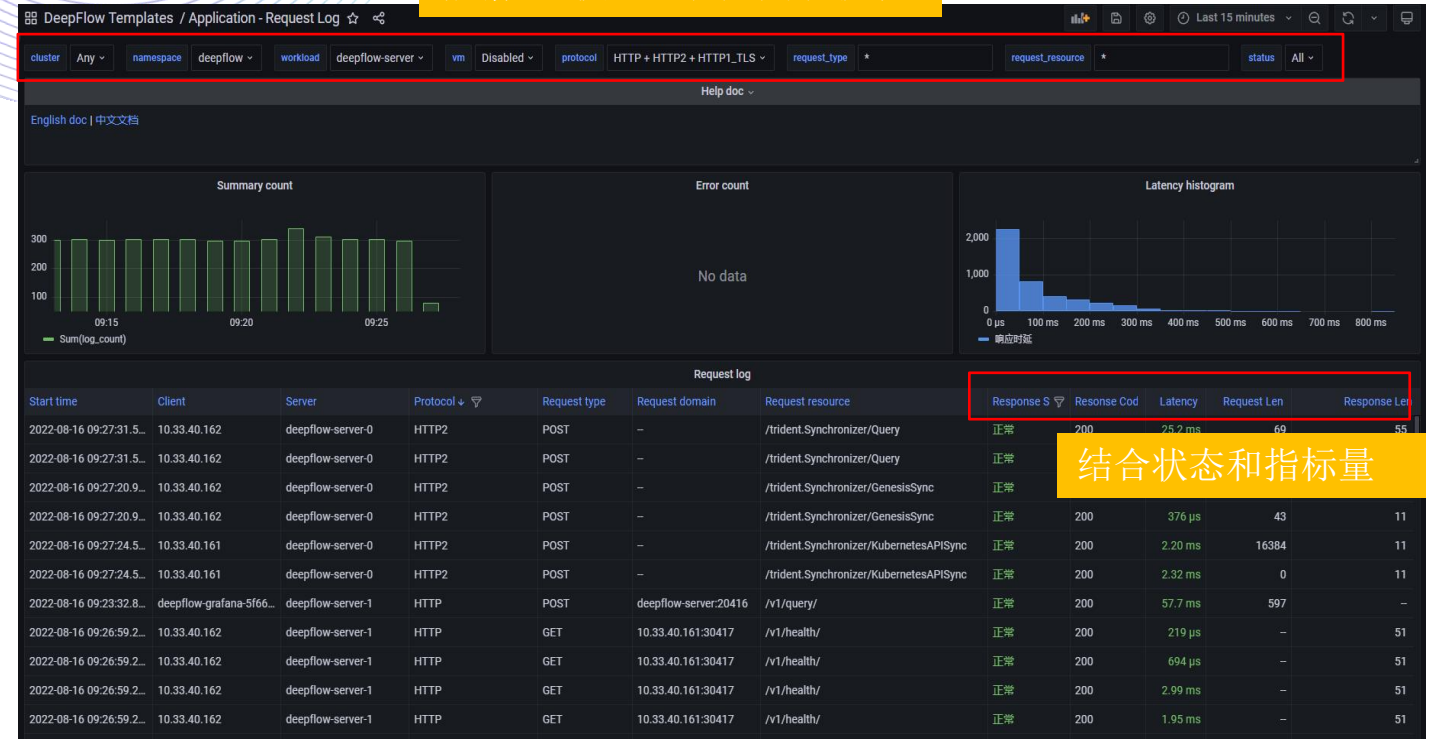
根据TAG快速过滤应用



https://ce-demo.deepflow.yunshan.net/d/Application_K8s_Pod/application-k8s-pod

应用调用日志-HTTP调用日志

根据TAG快速过滤应用和协议



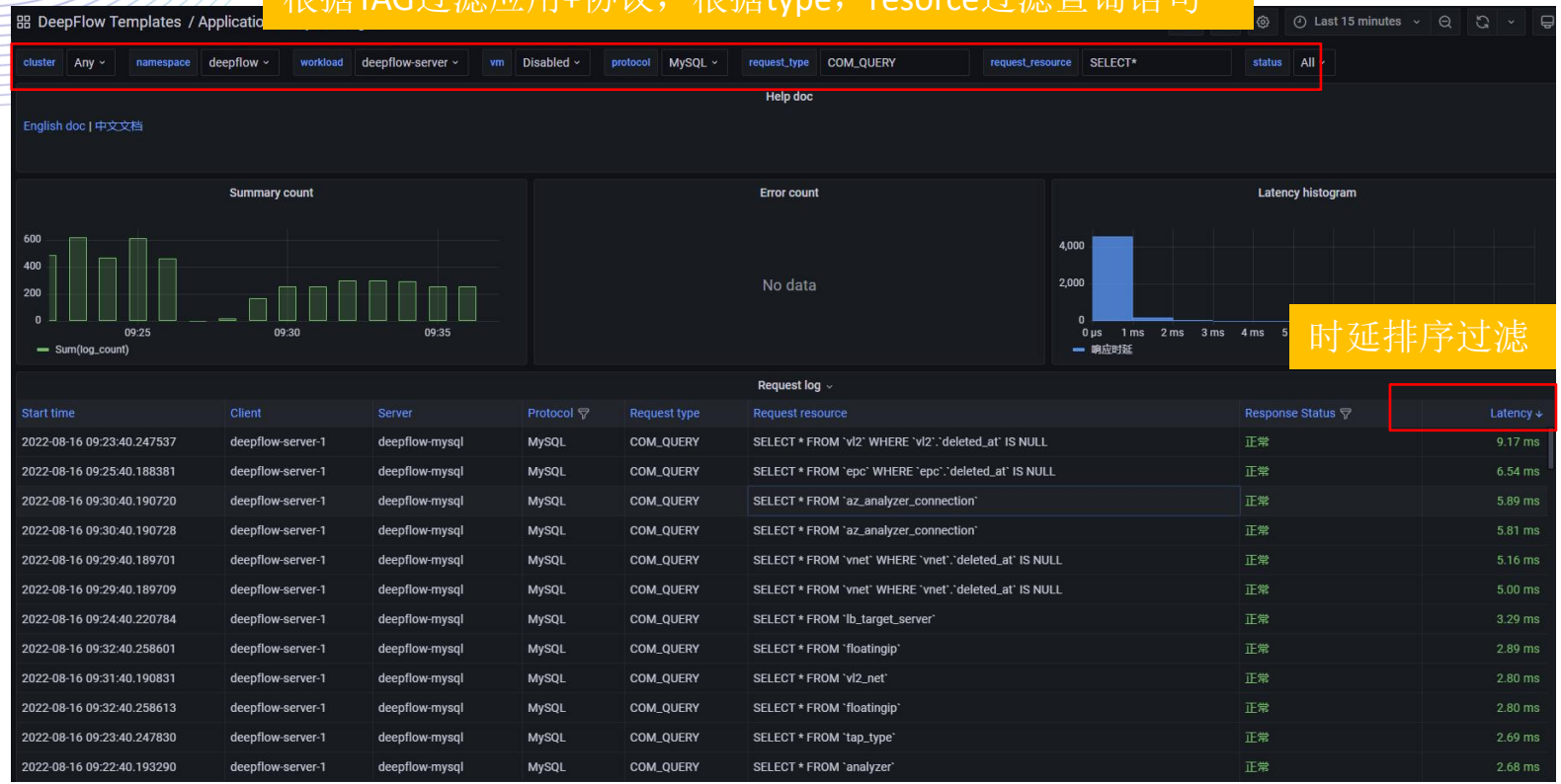
结合状态和指标量

AccessLog	DeepFlow 应用调用日志
remote_addr	client
remote_user	--
time_local	start time
request	request type request resource protocol version
status	response code
body_bytes_sent	request len
http_referer	自定义字段
http_user_agent	自定义字段
http_x_forwarded_for	自定义字段

https://ce-demo.deepflow.yunshan.net/d/Application_Request_Log

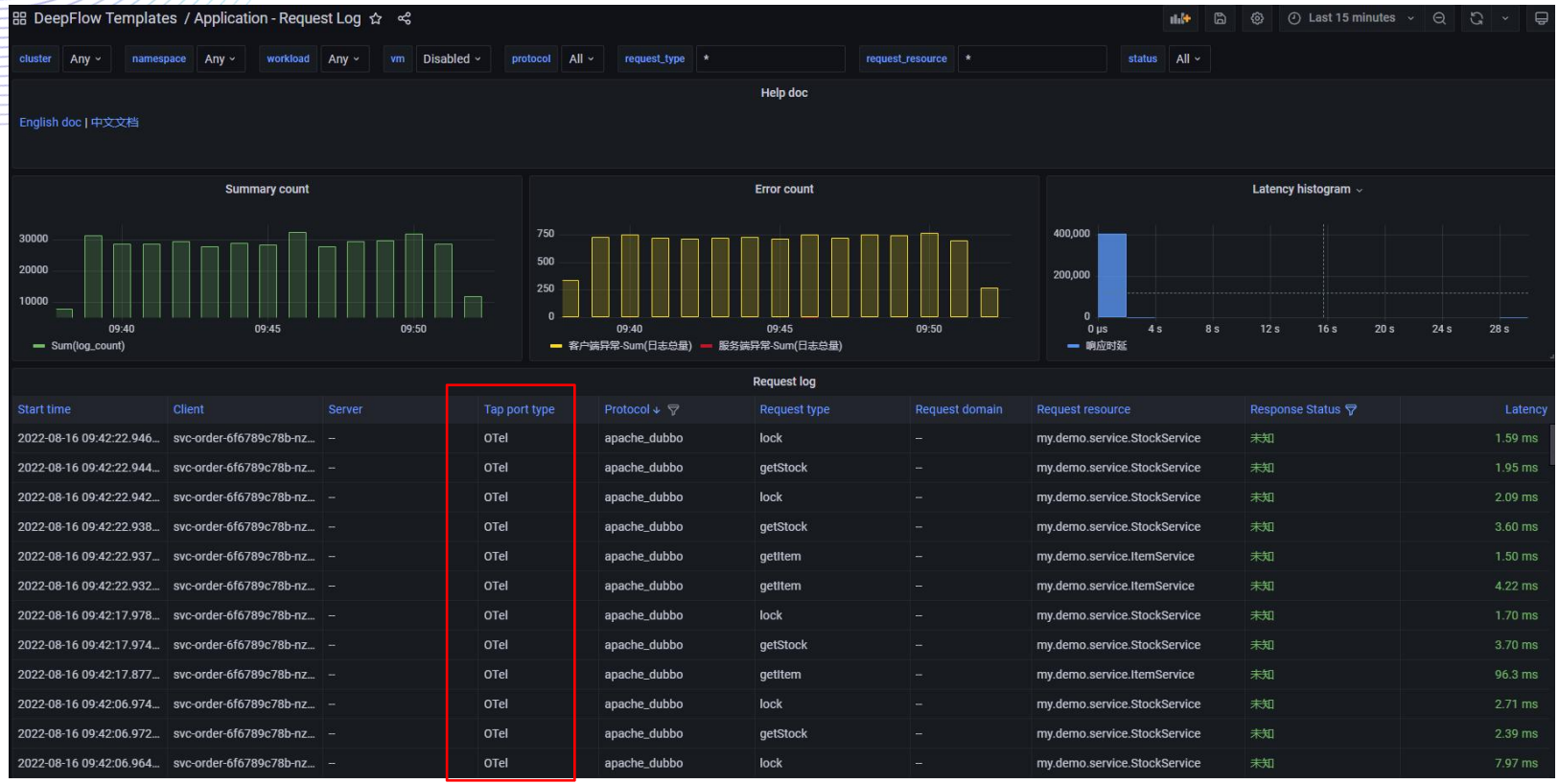
应用调用日志-MySQL慢查询日志

根据TAG过滤应用+协议，根据type，resorce过滤查询语句



https://ce-demo.deepflow.yunshan.net/d/Application_Request_Log

应用调用日志-分布式追踪的Span日志



Start time	Client	Server	Tap port type	Protocol	Request type	Request domain	Request resource	Response Status	Latency
2022-08-16 09:42:22.946...	svc-order-6f6789c78b-nz...	–	OTel	apache_dubbo	lock	–	my.demo.service.StockService	未知	1.59 ms
2022-08-16 09:42:22.944...	svc-order-6f6789c78b-nz...	–	OTel	apache_dubbo	getStock	–	my.demo.service.StockService	未知	1.95 ms
2022-08-16 09:42:22.942...	svc-order-6f6789c78b-nz...	–	OTel	apache_dubbo	lock	–	my.demo.service.StockService	未知	2.09 ms
2022-08-16 09:42:22.938...	svc-order-6f6789c78b-nz...	–	OTel	apache_dubbo	getStock	–	my.demo.service.StockService	未知	3.60 ms
2022-08-16 09:42:22.937...	svc-order-6f6789c78b-nz...	–	OTel	apache_dubbo	getItem	–	my.demo.service.ItemService	未知	1.50 ms
2022-08-16 09:42:22.932...	svc-order-6f6789c78b-nz...	–	OTel	apache_dubbo	getItem	–	my.demo.service.ItemService	未知	4.22 ms
2022-08-16 09:42:17.978...	svc-order-6f6789c78b-nz...	–	OTel	apache_dubbo	lock	–	my.demo.service.StockService	未知	1.70 ms
2022-08-16 09:42:17.974...	svc-order-6f6789c78b-nz...	–	OTel	apache_dubbo	getStock	–	my.demo.service.StockService	未知	3.70 ms
2022-08-16 09:42:17.877...	svc-order-6f6789c78b-nz...	–	OTel	apache_dubbo	getItem	–	my.demo.service.ItemService	未知	96.3 ms
2022-08-16 09:42:06.974...	svc-order-6f6789c78b-nz...	–	OTel	apache_dubbo	lock	–	my.demo.service.StockService	未知	2.71 ms
2022-08-16 09:42:06.972...	svc-order-6f6789c78b-nz...	–	OTel	apache_dubbo	getStock	–	my.demo.service.StockService	未知	2.39 ms
2022-08-16 09:42:06.964...	svc-order-6f6789c78b-nz...	–	OTel	apache_dubbo	lock	–	my.demo.service.StockService	未知	7.97 ms

https://ce-demo.deepflow.yunshan.net/d/Application_Request_Log

应用调用日志-全栈全链路追踪

https://ce-demo.deepflow.yunshan.net/d/Distributed_Tracing/distributed-tracing

内容目录

应用调用日志，自动采集HTTP/MySQL等多协议调用日志

网络流日志，丰富指标量及TAG增强网络可观测性

AutoLogging，基于 BPF/eBPF的自动日志采集能力

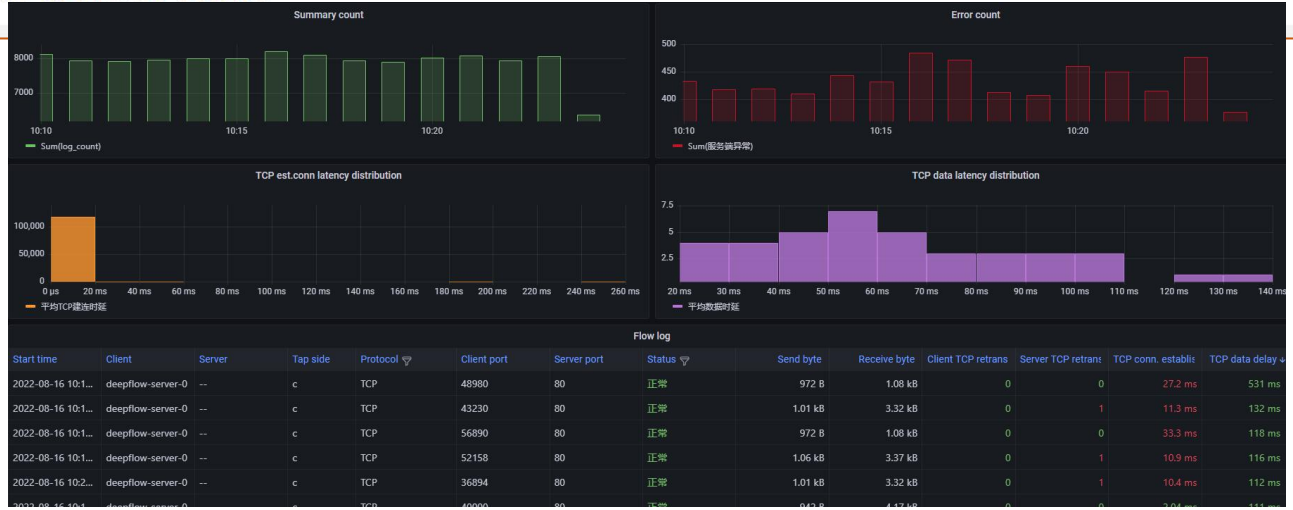
网络流日志-功能定义

功能介绍

阿里云

您可以捕获指定弹性网卡的流量，也可以捕获指定VPC或交换机的流量。如果选择为VPC或交换机创建流日志，则会捕获VPC和交换机中所有弹性网卡的流量，包括在开启流日志功能后新建的弹性网卡。

流日志功能捕获的流量信息会以流日志记录的方式写入日志服务（Log Service，简称LOG/原SLS）中。每条流日志记录会捕获特定捕获窗口中的特定五元组网络流，捕获窗口大约为10分钟，该段时间内流日志服务会先聚合数据，然后再发布流日志记录。流日志记录的字段信息如下表所示。

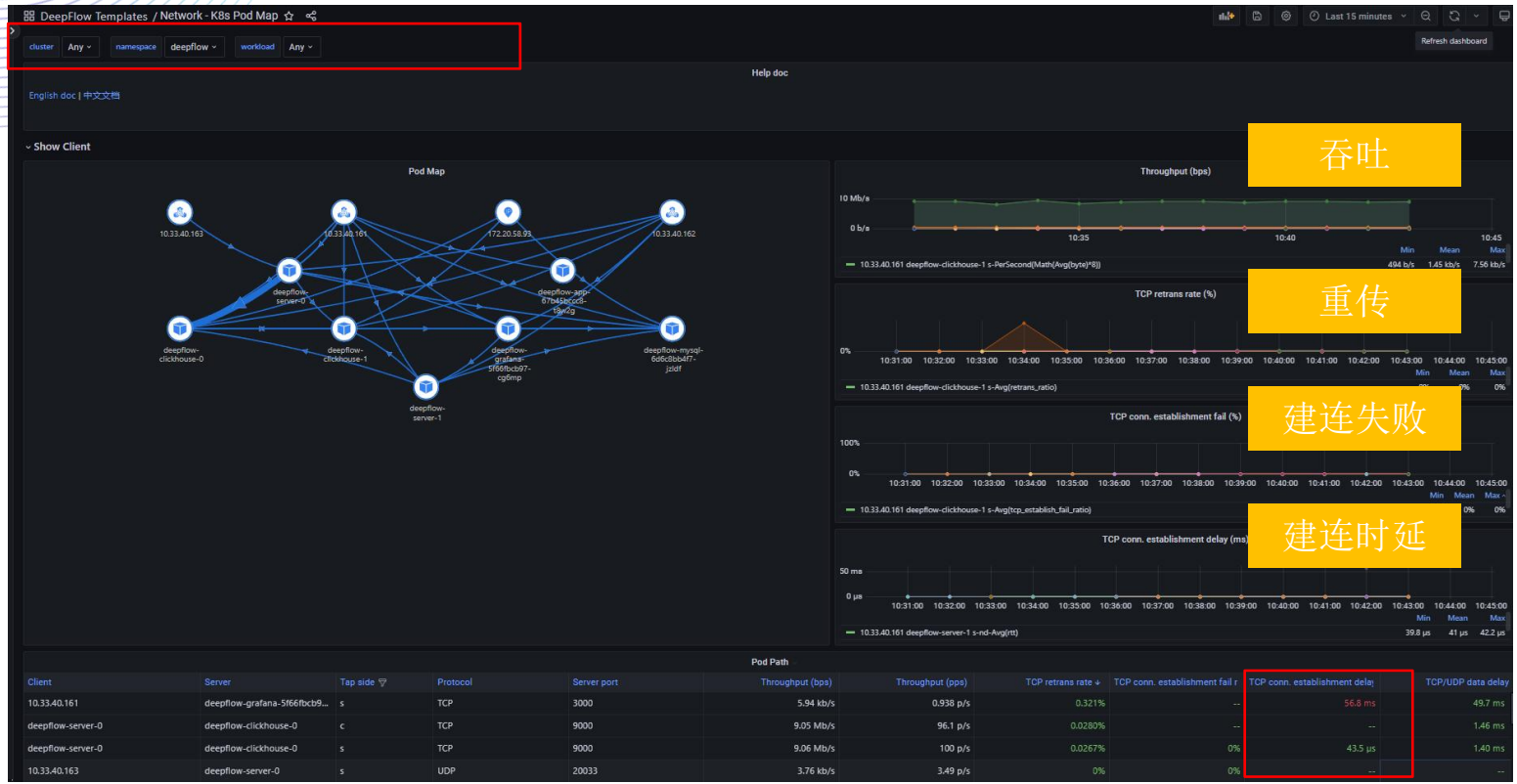


Start time	Client	Server	Tap side	Protocol	Client port	Server port	Status	Send byte	Receive byte	Client TCP retrans	Server TCP retrans	TCP conn. establis	TCP data delay
2022-08-16 10:1...	deepflow-server-0	--	c	TCP	48980	80	正常	972 B	1.08 kB	0	0	27.2 ms	531 ms
2022-08-16 10:1...	deepflow-server-0	--	c	TCP	43230	80	正常	1.01 kB	3.32 kB	0	1	11.3 ms	132 ms
2022-08-16 10:1...	deepflow-server-0	--	c	TCP	56890	80	正常	972 B	1.08 kB	0	0	33.3 ms	118 ms
2022-08-16 10:1...	deepflow-server-0	--	c	TCP	52158	80	正常	1.06 kB	3.37 kB	0	1	10.9 ms	116 ms
2022-08-16 10:2...	deepflow-server-0	--	c	TCP	36894	80	正常	1.01 kB	3.32 kB	0	1	10.4 ms	112 ms

网络流日志-DeepFlow与公有云对比

差异点	DeepFlow	公有云
捕获周期	1m	10m
捕获位置	VPC网络、容器网络、物理网络、系统接口（排期中）	VPC网络
五元组	支持	支持
隧道-TAG	支持（类型、外层IP/MAC等）	不支持
VPC网络-TAG	支持（VPC/VM/RDS/LB/NAT约20种）	支持（VPC/VM/Subnet）
容器网络-TAG	支持（cluster/ns/workload/service/pod约10种）	不支持
采集位置-TAG	支持（采集点/采集器/网卡/MAC等）	支持（网卡ID）
指标量-吞吐	支持（packet/byte/网络层载荷/传输层载荷等）	支持（packet/byte）
指标量-性能	支持（零窗/重传等）	不支持
指标量-时延	支持（建连/传输/协议栈等）	不支持
流状态	支持	不支持
包日志	TCP时序日志	不支持
日志状态	不支持（排期中）	支持
安全策略	不支持（排期中）	支持
计费	开源/SaaS免费	是

网络流日志-总览



吞吐

重传

建连失败

建连时延

https://ce-demo.deepflow.yunshan.net/d/Network_Flow_Log/network-flow-log

网络流日志-网络时延

Flow ID可将”应用调用日志”与”网络流日志“关联起来

Flow log

Start time	Client	Server	Flow Id	Tap side	Protocol	Client port	Server port	Status	Send byte	Receive byte	Client TCP retr	Server TCP retr	TCP conn. esta	TCP system de	TCP data delay
2022-08-16 1...	deepflow-gra...	--	6642470547387378923	c	TCP	48932	443	正常	1.99 kB	5.50 kB	0	0	48.9 ms	48.6 ms	33.5 ms
2022-08-16 1...	deepflow-ser...	--	6642470633286596974	c	TCP	60156	80	正常	972 B	1.08 kB	0	0	41.0 ms	40.5 ms	127 ms
2022-08-16 1...	deepflow-ser...	--	6642471354841109962	c	TCP	35512	80	正常	970 B	1.08 kB	0	0	41.6 ms	40.5 ms	89.8 ms
2022-08-16 1...	deepflow-ser...	--	6642470392768425916	c	TCP	41852	80	正常	972 B	832 B	0	0	39.8 ms	40.0 ms	113 ms
2022-08-16 1...	deepflow-ser...	--	6642471114322938983	c	TCP	45962	80	正常	919 B	837 B	0	0	34.4 ms	36.9 ms	59.9 ms
2022-08-16 1...	deepflow-ser...	--	6642471114322938970	c	TCP	38018	80	正常	970 B	1.08 kB	0	0	35.8 ms	35.1 ms	112 ms
2022-08-16 1...	deepflow-ser...	--	6642471114322938953	c	TCP	37996	80	正常	901 B	1.29 kB	0	0	35.5 ms	35.0 ms	118 ms
2022-08-16 1...	deepflow-ser...	--	6642470152250254891	c	TCP	37194	80	正常	974 B	832 B	0	0	35.4 ms	34.1 ms	83.6 ms
2022-08-16 1...	deepflow-ser...	--	6642470152250254878	c	TCP	37184	80	正常	901 B	1.29 kB	0	0	33.4 ms	33.9 ms	98.1 ms
2022-08-16 1...	deepflow-ser...	--	6642471354841109974	c	TCP	48254	80	正常	917 B	837 B	0	0	34.9 ms	33.9 ms	63.9 ms
2022-08-16 1...	deepflow-ser...	--	6642470873804768008	c	TCP	35182	80	正常	970 B	1.08 kB	0	0	34.4 ms	33.8 ms	81.5 ms
2022-08-16 1...	deepflow-ser...	--	6642470392768425936	c	TCP	48746	80	正常	919 B	829 B	0	0	33.8 ms	33.5 ms	66.3 ms
2022-08-16 1...	deepflow-ser...	--	6642470873804767985	c	TCP	35170	80	正常	899 B	1.29 kB	0	0	33.5 ms	33.3 ms	97.0 ms

网络时延=建连时延+协议栈处理时延+网络传输时延

https://ce-demo.deepflow.yunshan.net/d/Network_Flow_Log/network-flow-log

网络流日志-流状态异常日志

status (状态：由流结束类型决定。正常：正常结束、周期性上报。客户端异常：客户端SYN结束、客户端重置、客户端半关、客户端端口复用、客户端其他重置。服务端异常：服务端重置、连接超时、服务端半关、服务端SYN结束、服务端直接重置、服务端队列溢出、服务端其他重置。未知：其他结束方式。)

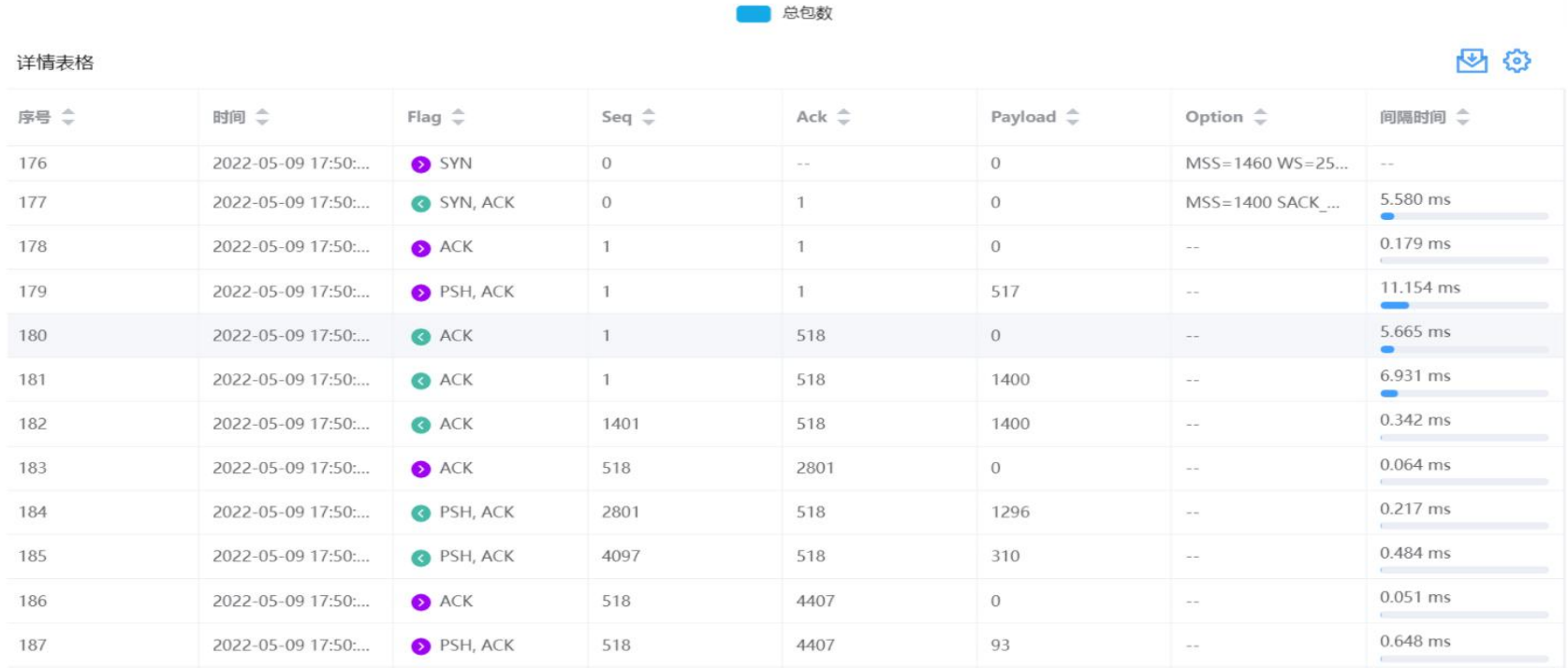
对状态过滤，追踪异常流

Flow log

Start time	Client	Server	Flow Id	Tap side	Protocol	Client port	Server port	Status	Send byte	Receive byte	Client TCP retr	Server TCP retr	TCP conn. esta	TCP system de	TCP data delay
2022-08-16 1...	deepflow-gra...	--	6642470547387378923	c	TCP	48932	443	正常	1.99 kB	5.50 kB	0	0	48.9 ms	48.6 ms	33.5 ms
2022-08-16 1...	deepflow-ser...	--	6642470633286596974	c	TCP	60156	80	正常	972 B	1.08 kB	0	0	41.0 ms	40.5 ms	127 ms
2022-08-16 1...	deepflow-ser...	--	6642471354841109962	c	TCP	35512	80	正常	970 B	1.08 kB	0	0	41.6 ms	40.5 ms	89.8 ms
2022-08-16 1...	deepflow-ser...	--	6642470392768425916	c	TCP	41852	80	正常	972 B	832 B	0	0	39.8 ms	40.0 ms	113 ms
2022-08-16 1...	deepflow-ser...	--	6642471114322938983	c	TCP	45962	80	正常	919 B	837 B	0	0	34.4 ms	36.9 ms	59.9 ms
2022-08-16 1...	deepflow-ser...	--	6642471114322938970	c	TCP	38018	80	正常	970 B	1.08 kB	0	0	35.8 ms	35.1 ms	112 ms
2022-08-16 1...	deepflow-ser...	--	6642471114322938953	c	TCP	37996	80	正常	901 B	1.29 kB	0	0	35.5 ms	35.0 ms	118 ms
2022-08-16 1...	deepflow-ser...	--	6642470152250254891	c	TCP	37194	80	正常	974 B	832 B	0	0	35.4 ms	34.1 ms	83.6 ms
2022-08-16 1...	deepflow-ser...	--	6642470152250254878	c	TCP	37184	80	正常	901 B	1.29 kB	0	0	33.4 ms	33.9 ms	98.1 ms
2022-08-16 1...	deepflow-ser...	--	6642471354841109974	c	TCP	48254	80	正常	917 B	837 B	0	0	34.9 ms	33.9 ms	63.9 ms
2022-08-16 1...	deepflow-ser...	--	6642470873804768008	c	TCP	35182	80	正常	970 B	1.08 kB	0	0	34.4 ms	33.8 ms	81.5 ms
2022-08-16 1...	deepflow-ser...	--	6642470392768425936	c	TCP	48746	80	正常	919 B	829 B	0	0	33.8 ms	33.5 ms	66.3 ms
2022-08-16 1...	deepflow-ser...	--	6642470873804767985	c	TCP	35170	80	正常	899 B	1.29 kB	0	0	33.5 ms	33.3 ms	97.0 ms

https://ce-demo.deepflow.yunshan.net/d/Network_Flow_Log/network-flow-log

网络流日志-TCP时序日志



Demo

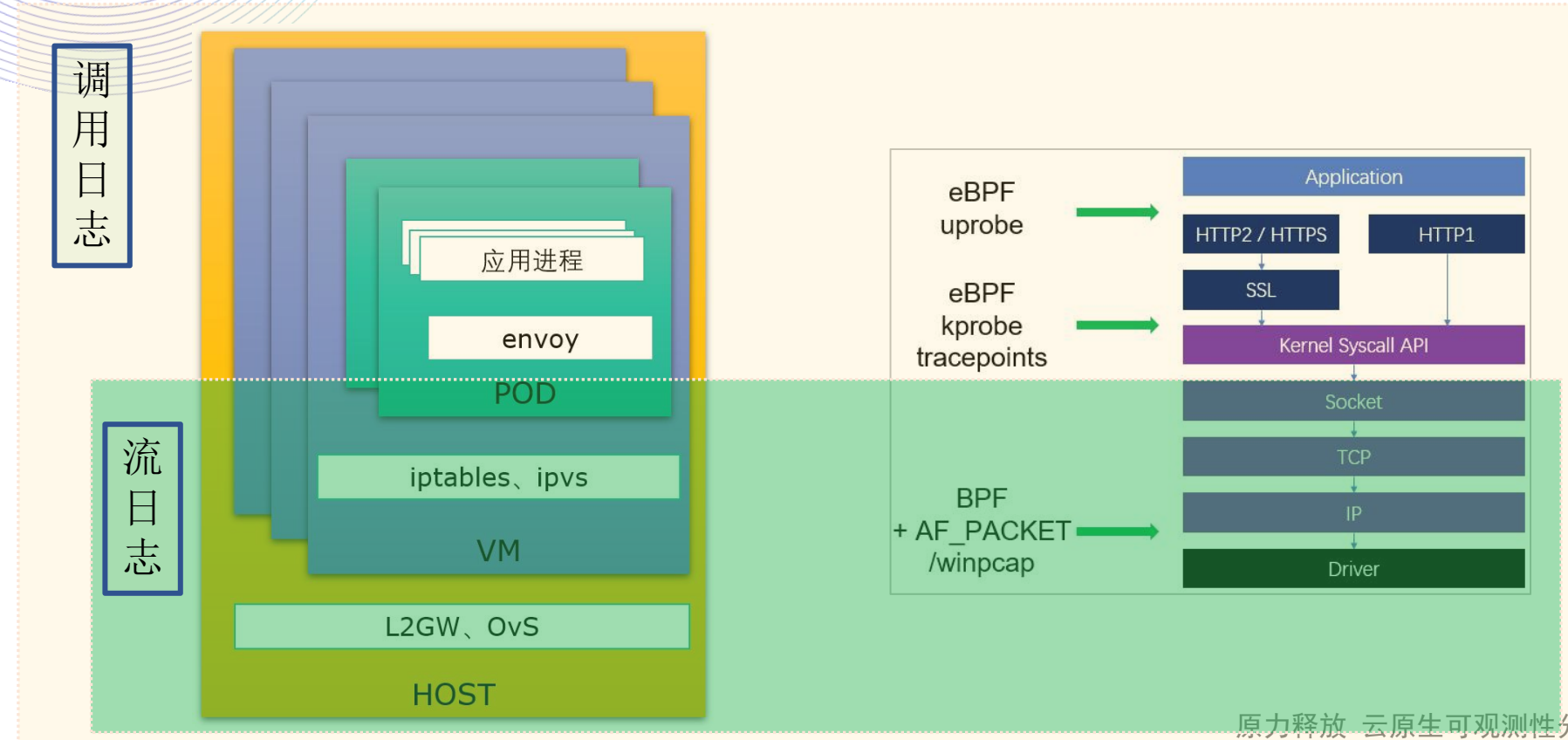
内容目录

应用调用日志，自动采集HTTP/MySQL等多协议调用日志

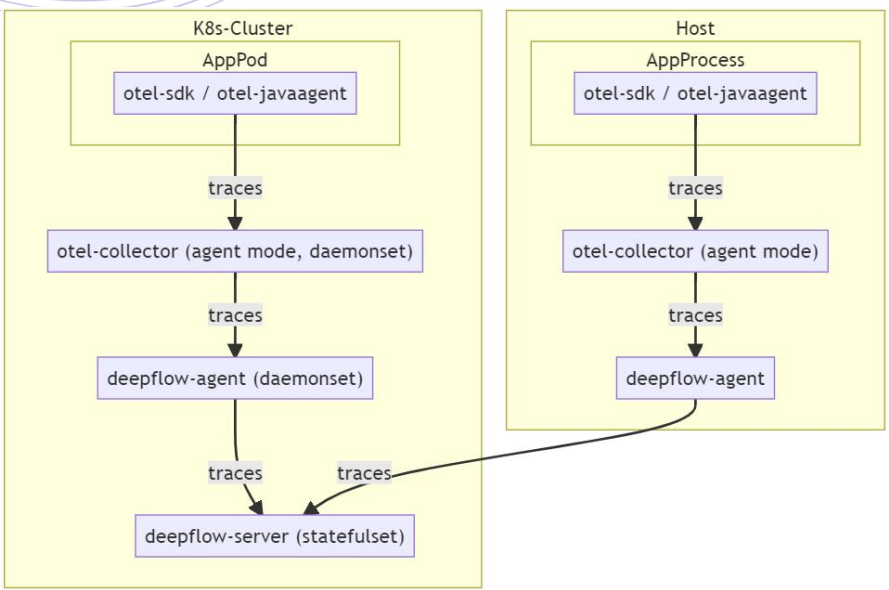
网络流日志，丰富指标量及TAG增强网络可观测性

AutoLogging，基于 BPF/eBPF的自动日志采集能力

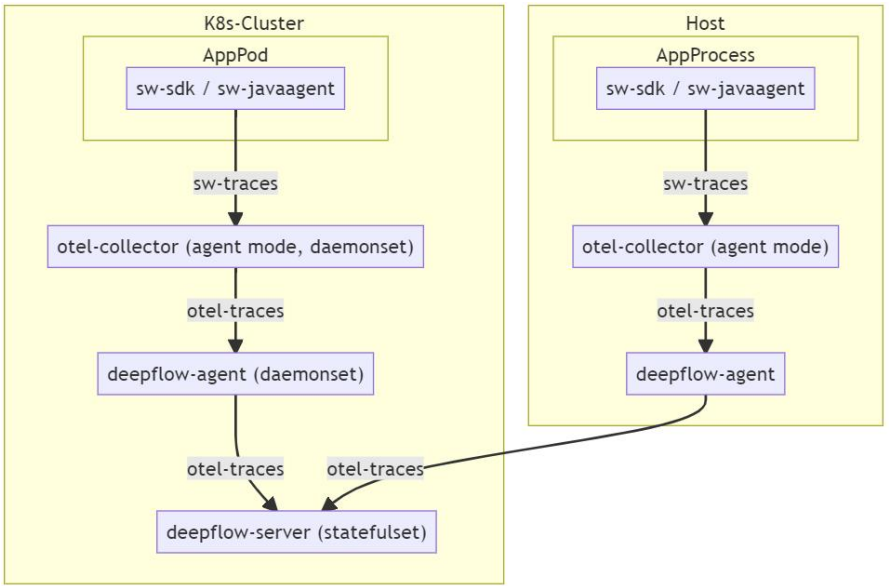
AutoLogging-采集



AutoLogging-采集

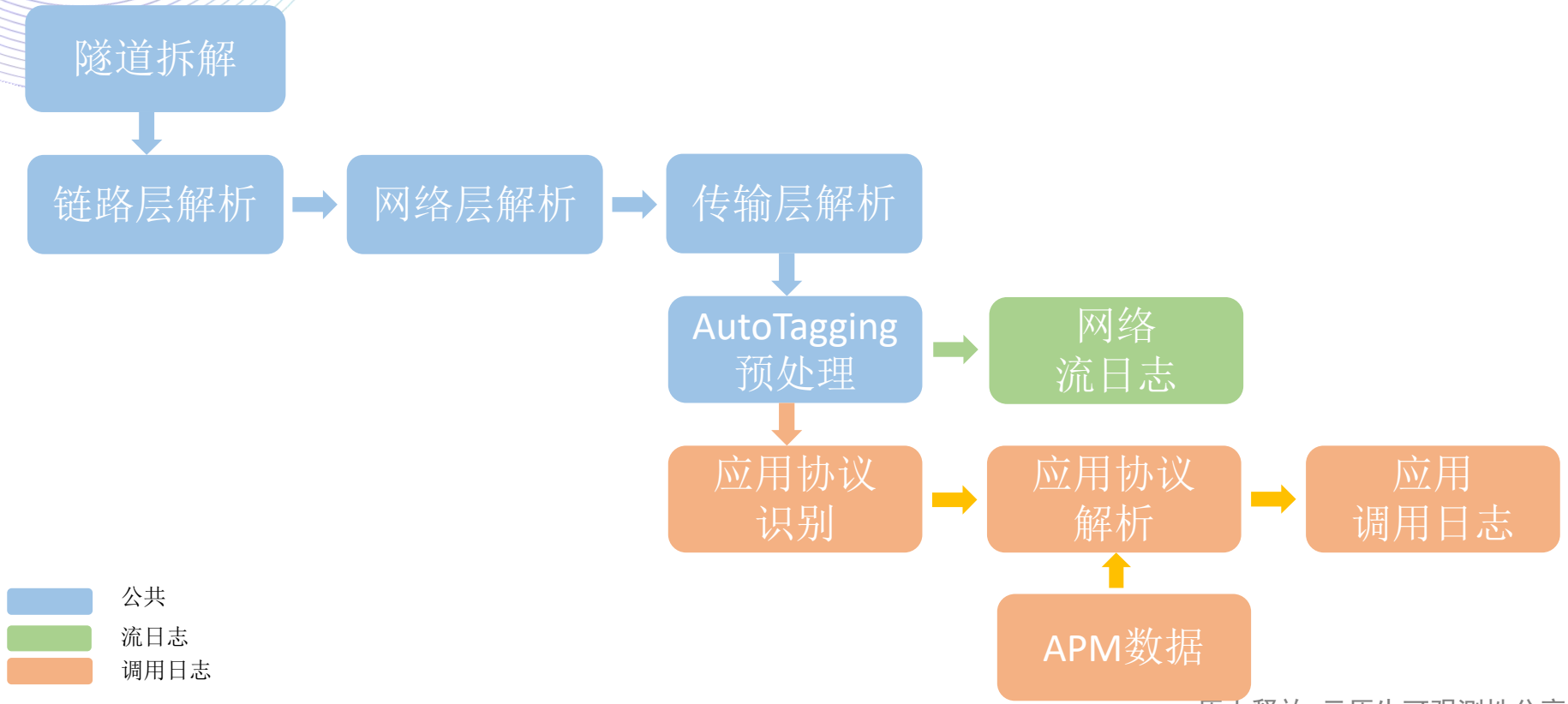


OpenTelemetry



OpenTelemetry + SkyWalking

AutoLogging-处理



应用调用日志-协议扩展

```rust
#[derive(Default)]
2 implementations
struct AppLogs {
    dns: DnsLog,
    http: HttpLog,
    mysql: MysqlLog,
    redis: RedisLog,
    dubbo: DubboLog,
    kafka: KafkaLog,
    mqtt: MqttLog,
}
```

应用调用日志映射

```rust
impl L7LogParse for HttpLog {
    fn parse(
        &mut self,
        payload: &[u8],
        proto: IpProtocol,
        direction: PacketDirection,
    ) -> Result<AppProtoHead> {
        if proto != IpProtocol::Tcp {
            return Err(Error::InvalidIpProtocol);
        }
        self.reset_logs();

        self.parse_http_v1(payload, direction)
            .or(self.parse_http_v2(payload, direction))?;

        Ok(AppProtoHead {
            proto: self.get_l7_protocol(),
            msg_type: self.msg_type,
            status: self.status,
            code: self.status_cod
            rrt: 0,
            version: 0,
        })
    }

    fn info(&self) -> AppProtoLog
        if self.info.version == "
            return AppProtoLogsIn
        }
        if self.is_https {
            return AppProtoLogsIn
        }
        AppProtoLogsInfo::HttpV1(
    }
}
```

应用解析协议

```rust
pub trait L7LogParse: Send + Sync {
    fn parse(
        &mut self,
        payload: &[u8],
        proto: IpProtocol,
        direction: PacketDirection,
    ) -> Result<AppProtoHead>;
    fn info(&self) -> AppProtoLogsInfo;
}
```

```rust
#[enum_dispatch(L7FlowPerfTable)]
pub trait L7FlowPerf {
    fn parse(&mut self, packet: &MetaPacket, flow_id: u64) -> Result<()>;
    fn data_updated(&self) -> bool;
    fn copy_and_reset_data(&mut self, l7_timeout_count: u32) -> FlowPerfStats;
    fn app_proto_head(&mut self) -> Option<(AppProtoHead, u16)>;
}

#[enum_dispatch]
pub enum L7FlowPerfTable {
    DnsPerfData,
    KafkaPerfData,
    MqttPerfData,
    RedisPerfData,
    DubboPerfData,
    MysqlPerfData,
    HttpPerfData,
}
```

应用RED指标计算

github.com/deepflowys/deepflow

未来迭代的方向

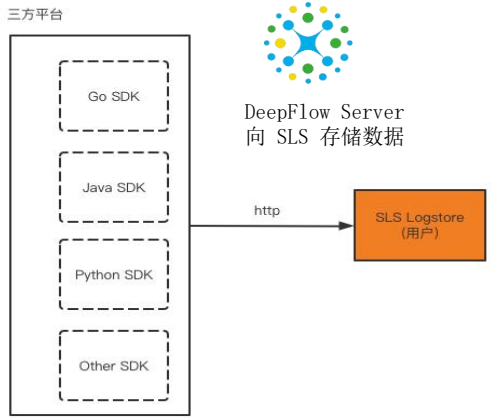
高度自动化的可观测性，即将由 DeepFlow 带给 SLS 用户

DeepFlow®

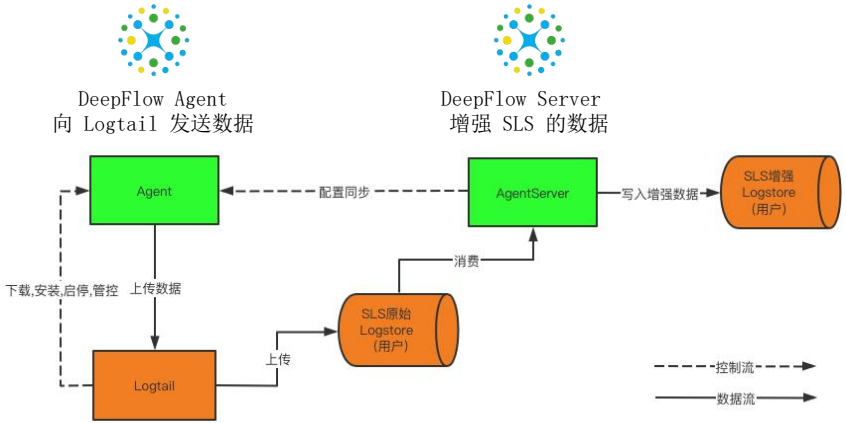
AutoMetrics | AutoTracing | SmartEncoding | AutoTagging

低开销 | 零插码 | 全景访问关系 | 全栈性能指标 | 无盲点追踪

跨云与混合云场景



阿里云公共云场景



开始构建可观测性

Cloud

免费试用

Community

下载DeepFlow源码

Enterprise

咨询专家

我们在招聘，HR 微信：holidayxd